Math100B - HW #3

Jay Ser

2026.01.23

Even though they are more or less the same things, I prefer thinking about ideals rather than quotient rings, so here are some propositions.

Claim 1. *R/I is an integral domain $\iff$ I is a prime ideal*

Proof of Claim 1.

$$\begin{aligned} I \text{ is a prime ideal} &\iff \forall ab \in I, a \in I \text{ or } b \in I \\ &\iff \forall \bar{a}\bar{b} \in R/I,\ \bar{a}\bar{b} = 0 \implies \bar{a} = 0 \text{ or } \bar{b} = 0 \\ &\iff R/I \text{ is an integral domain} \end{aligned}$$

□

Claim 2. *R/I is a field $\iff$ I is a maximal ideal*

Proof of Claim 2. By the definition of a field, namely, that every nonzero element has a multiplicative inverse, it is clear that a ring has only two ideals – the zero ring and the entire ring – if and only if the ring is a field. Now, via the Correspondence Theorem,

$$\begin{aligned} R/I \text{ is a field} &\iff 0 \text{ and } R/I \text{ are the only ideals in } R/I \\ &\iff \text{in } R, \text{ the only ideal properly containing } I \text{ is } R \\ &\iff I \text{ is a max ideal in } R \end{aligned}$$

□

1.

Consider the substitution homomorphism

$$\varphi : R[x] \to R;\ x \mapsto a,\ \varphi|_R = \mathrm{id}$$

Clearly, $x - a \in \ker\varphi$, so $\langle x - a\rangle \subset \ker\varphi$. Take any $f(x) \in \ker\varphi$. Because $x - a$ is monic, it is possible to divide $f(x)$ with remainder by $x - a$ to get

$$f(x) = q(x)(x - a) + r, \text{ where } r = c \text{ for some constant } c \in R$$

Because $f(x), x - a \in \ker\varphi$, $r \in \ker\varphi$. So $\varphi(f(x)) = \varphi(r) = r = c = 0$, which means $r = 0$. In other words, $x - a \mid f(x)$, which shows $\ker\varphi = \langle x - a\rangle$. Finally, φ is clearly surjective since it is the identity function on constant polynomials. Thus, by the First Isomorphism Theorem, $R[x]/\langle x - a\rangle \cong R$.

2.

Suppose n is a perfect square, say $n = a^2$ for some $a \in \mathbb{Z}$. Then $\sqrt{n} = a$, so $\mathbb{Q}[\sqrt{n}]$ is just $\mathbb{Q}[a] = \mathbb{Q}$. Meanwhile, $\mathbb{Q}[x]/\langle x^2 - n\rangle$ is not even an integral domain: $x^2 - n = (x+a)(x-a)$; namely, $x^2 - n$ divides the product $(x+a)(x-a)$. However, $x^2 - n$ clearly does not divide $x + a$ nor $x - a$ because $\mathbb{Q}[x]$ is an integral domain (see Q3) and $x^2 - n$ has a greater degree than both $x + a$ and $x - a$. This shows that the principal ideal $\langle x^2 - n\rangle$ is not a prime ideal, and hence $\mathbb{Q}[x]/\langle x^2 - n\rangle$ is not an integral domain. $\mathbb{Q}[\sqrt{n}] = \mathbb{Q}$, on the other hand, is an integral domain, so $\mathbb{Q}[a] \neq \mathbb{Q}[x]/\langle x^2 - n\rangle$.

To show the reverse direction, suppose n is not a perfect square. Then $x^2 - n$ is the least degree polynomial in $\mathbb{Q}[x]$ that has $\sqrt{n}$ as a root (clearly no linear polynomial in $\mathbb{Q}[x]$ has $\sqrt{n}$ as a root, since $\sqrt{n} \notin \mathbb{Q}$). Now consider the substitution homomorphism

$$\varphi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{n}];\ x \mapsto \sqrt{n},\ \varphi|_{\mathbb{Q}} = \mathrm{id}$$

Clearly $x^2 - n \in \ker\varphi$, so $\langle x^2 - n\rangle \subset \ker\varphi$. Next, take any $f(x) \in \ker\varphi$. Since $\mathbb{Q}$ is a field and therefore $\mathbb{Q}[x]$ is a Euclidean Domain, divide $f(x)$ with remainder by $x^2 - n$ to obtain

$$f(x) = q(x)(x^2 - n) + r(x),\ \text{where } r(x) = 0 \text{ or } \deg(r) < 2$$

Suppose $r(x) \neq 0$. $f(x), x^2 - n \in \ker\varphi$, so $r(x) \in \ker\varphi$ as well. So $\varphi(f(x)) = \varphi(r(x)) = 0$. But the image of $r(x)$ under the substitution map cannot be zero because $r(x)$ has degree less than $x^2 - n$, the latter being the least-degree polynomial that has $\sqrt{n}$ as a root, thus yielding a contradiction. As such, $r(x) = 0$; $x^2 - n \mid f(x)$. This shows $\langle x^2 - n\rangle = \ker\varphi$. Finally, it is clear that the map is surjective because 1, $\sqrt{n}$ form a basis for the image of $\varphi(\mathbb{Q}[x])$, which generate the entirity of $\mathbb{Q}[\sqrt{n}]$. Thus, by the First Isomorphism Theorem, $\mathbb{Q}[x]/\langle x^2 - n\rangle \cong \mathbb{Q}[\sqrt{n}]$.

3.

Take any $f(x), g(x) \in R[x] \setminus 0$ and let $f(x) = a_n x^n + \ldots + a_0$, $g(x) = b_m x^m + \ldots + b_0$, where $a_n \neq 0$ and $b_m \neq 0$. Then $f(x)g(x) = a_n b_m x^{n+m}+$ lower degree terms. Because R is an integral domain, $a_n b_m \neq 0$, so $f(x)g(x) \neq 0$ as well. This shows that $R[x]$ is an integral domain.

Particularly, the proof above shows that $\deg(fg) = \deg(f) + \deg(g)$. Because every nonzero element of $\langle f(x)\rangle$ is of the form $f(x)g(x)$ for $g(x) \neq 0$, every element in the ideal generated by the polynomial f has a degree greater or equal to the degree of f.

4.

(a)

Let $I := \langle 2x - 6, x - 10\rangle$. Let's directly identify $\mathbb{Z}[x]/I$. First, following my solution to Q1, the substitution map

$$\varphi : \mathbb{Z}[x] \to \mathbb{Z};\ x \mapsto 10,\ \varphi|_{\mathbb{Z}} = id$$

gives the isomorphism $\mathbb{Z}[x]/\langle x - 10\rangle \cong \mathbb{Z}$. $\ker\varphi = \langle x - 10\rangle \subset I$, so by the Correspondence Theorem, $I \mapsto \langle 2\overline{x} - 6\rangle = \langle 20 - 6\rangle = \langle 14\rangle$ in $\mathbb{Z}$. 14 is not a prime number, so $\mathbb{Z}/14\mathbb{Z}$ is not an integral domain by HW#2. The Correspondence Theorem says $\mathbb{Z}[x]/I \cong \mathbb{Z}/\langle 14\rangle$, so $\mathbb{Z}[x]/I$ is not an integral domain.

(b)

$\mathbb{Z}[x]/\langle x^2+x\rangle$ is not an integral domain because $\langle x^2+x\rangle$ is not a prime ideal in $\mathbb{Z}[x]$: $x^2+x = x(x+1) \in \langle x^2+x\rangle$, but x and $x+1$ are both not in $\langle x^2+x\rangle$ because x and $x+1$ are both of lower degree than x^2+x and $\mathbb{Z}[x]$ is an integral domain; hence, x^2+x cannot divide x or $x+1$.

5.

(a)

1 is not a zerodivisor: $\forall a \neq 0 \in R$, $1a = a \neq 0$. Now, the result follows by (b)

(b)

Suppose φ is not injective: $\exists a \neq b \in R$ such that $a + \langle f\rangle = b + \langle f\rangle$ in $R[x]/(f)$. The latter condition is equivalent to $a - b \in (f)$ in $R[x]$. Now, since $a \neq b$ in R, $a - b \neq 0$ in $R[x]$. Furthermore, $\forall g \in R[x]$, $\deg(fg) \geq \deg(f)$ since the leading coefficient of f is not a zerodivisor. So no nonzero constant is in $\langle f\rangle$, which contradicts $a - b \in \langle f\rangle$. This shows that φ is injective.

(c)

Consider

$$\varphi : \mathbb{Z}/12\mathbb{Z} \to (\mathbb{Z}/12\mathbb{Z})[x]/\langle 3x-1\rangle$$

$4(3x-1) = 12x - 4 \equiv 8 \pmod{12}$, so $8 \in \langle 3x-1\rangle$ in $(\mathbb{Z}/12\mathbb{Z})[x]$. Denote $I = \langle 3x-1\rangle$. Then $9 + I = 1 + I$ since $(9-1) + I = 8 + I = 0 + I$. In other words, $9 \neq 1$ in $\mathbb{Z}/12\mathbb{Z}$, but they map to the same value in $(\mathbb{Z}/12\mathbb{Z})[x]/\langle 3x-1\rangle$, so φ is not injective.

6.

Suppose $x^2 - a$ has no root. This is equivalent to saying that $x^2 - a$ has no linear factor. But because $x^2 - a$ is a polynomial of degree 2 in the integral domain $F[x]$, $x^2 - a$ having no linear factor means $x^2 - a$ is irreducible in $F[x]$. $F[x]$ is a Euclidean Domain. Namely, it is a Principal Ideal Domain, so $x^2 - a$ generates a maximal ideal in $F[x]$. This shows that $F[x]/(x^2 - a)$ is a field.

Conversely, if $x^2 - a$ does have a root, say $f(\alpha) = 0$, then

$$x^2 - a = (x - \alpha)(x - \beta)$$

for some $\beta \in F$. Because $F[x]$ is an integral domain, neither $x - \alpha$ nor $x - \beta$ are in $\langle x^2 - a\rangle$ even though $(x-\alpha)(x-\beta) \in \langle x^2 - a\rangle$. So $\langle x^2 - a\rangle$ is not a prime ideal, which means $F[x]/\langle x^2 - a\rangle$ is not even an integral domain; then certainly, $F[x]/\langle x^2 - a\rangle$ is not a field.

7.

(a)

Consider the canonical homomorphism

$$\pi : R[x] \to R[x]/\langle ax - 1\rangle$$

By definition, $\ker \pi = \langle ax - 1\rangle$, so $ax - 1 \mapsto 0$. Using bar notation to denote the image,

$$\overline{ax} - 1 = 0$$

So $\overline{a}$ indeed does have an inverse in the quotient; namely $\overline{a}^{-1} = \overline{x}$.

(b)

Consider the map Take any $f(x) = b_n x^n + + b_{n-1}x^{n-1} \ldots + b_1 x + b_0 \in R[x]$. Under the projection map to $R[x]/\langle ax - 1\rangle$,

$$\begin{aligned} f(x) &\mapsto b_n a^{-n} + b_{n-1}a^{-n+1} + \ldots + b_1 a^{-1} + b_0 \\ &= a^{-n}(b_n + b_{n-1}a + \ldots + b_1 a^{n-1} + b_0 a^n) \\ &= a^{-n} b \end{aligned}$$

where bars have been dropped for convenience and where $b = b_n + b_{n-1}a + \ldots + b_1 a^{n-1} + b_0 a^n \in R$.

(c)

Suppose $a^n b = 0$. Then $\bar{a}^n \bar{b} = \bar{0}$. Multiplying both sides by $\bar{x}^n$, $\bar{b} = \bar{0}$. So $b \in \ker \varphi$.

Conversely, suppose $b \in \ker \varphi$. Now, by definition of ϕ, $\ker \varphi = \ker \pi \cap R$, where π is the canonical proejction map. So $b \in \ker \pi = \langle 2x = 1\rangle$, i.e.,

$$b = (ax - 1)(c_n x^n + c_{n-1}x^{n-1} + \ldots + c_0)$$

Then

$$\begin{aligned} c_0 &= -b \\ ac_0 - c_1 &= 0 \\ ac_1 - c_2 &= 0 \\ &\vdots \\ ac_{n-1} - c_n &= 0 \\ ac_n &= 0 \end{aligned}$$

Inducting down the system of equations, $a^{n+1} b = 0$

(d)

The result follows from (c). By the First Isomorphism Theorem, $\varphi(S) \cong R/\ker\varphi$. If $S = 0$, then $\varphi(S) = 0$, which forces $\ker\varphi = R$. Thus $\forall b \in R$, $a^n b = 0$ for some $n \in \mathbb{Z}_{\geq 0}$. Namely, $\exists m \in \mathbb{Z}_{\geq 0}$ such that $a^m a = 0$, or in other words, $a^{m+1} = 0$. So a is nilpotent.

Conversely, if a is nilpotent, say $a^k = 0$, then $\forall b \in R$, $ba^k = 0$. Hence $\ker\varphi = R$. Extending the result to the substition map, which by definition of φ is equivalent to the canonical projection map, there is a homomorphism

$$\Phi : R[x] \to S;\ x \mapsto \bar{a}^{-1},\ \Phi|_R = \varphi$$

But because φ is just the zero map, Φ is also just the zero map, i.e., $\ker\Phi = \Phi$. Furthermore, Φ is the canonical projection map, so it is surjection. Thus, by the First Isomorphism Theorem,

$$R[x]/\ker\Phi \cong 0 \cong S$$

and hence $S = 0$.
** note that because $0 = 1$ in the zero ring, the homomorphisms φ and Φ still observe the $1 \mapsto 1$ rule for ring homomorphisms